

Claims

- 1 1. A method comprising:
2 generating a cipher stream based on a first key for encrypted streamed
3 content;
4 generating a second cipher stream based on a second key to re-encrypt the
5 streamed content;
6 receiving the encrypted streamed content;
7 simultaneously decrypting and re-encrypting the encrypted content using a
8 combination of the first and the second cipher streams;
9 conveying the re-encrypted content to a sink.
- 1 2. The method of Claim 1, wherein simultaneously decrypting and re-
2 encrypting the encrypted streamed content comprises exclusive OR-ing the encrypted
3 streamed content with the cipher stream combination.
- 1 3. The method of Claim 1, wherein the cipher stream combination comprises
2 a result of exclusive OR-ing the first and second cipher streams.
- 1 4. The method of Claim 3, wherein the first key and the second key have
2 symmetric agreement.
- 1 5. The method of Claim 1, further comprising receiving one or more of the
2 first key and the second key over a secure authenticated channel.
- 1 6. The method of Claim 5, wherein receiving a key over a secure
2 authenticated channel comprises receiving the key from a sales server.
- 1 7. The method of Claim 5, wherein the secure authenticated channel
2 comprises an Internet connection.

096396390-082901
T06290-082901

1 8. The method of Claim 5, wherein the secure authenticated channel
2 comprises a telephone line.

1 9. The method of Claim 1, further comprising conveying the second key to
2 the sink to enable the sink to decrypt the re-encrypted content.

1 10. The method of Claim 1, wherein the encrypted streamed content is
2 publicly available and encrypted with a public key and wherein the first key is a locally
3 available private key.

1 11. The method of Claim 1, wherein the encrypted content is a broadcasted
2 entertainment program.

1 12. A machine-readable medium having stored thereon data representing
2 sequences of instructions which, when executed by a machine, cause the machine to
3 perform operations comprising:

4 generating a cipher stream based on a first key for encrypted streamed
5 content;

6 generating a second cipher stream based on a second key to re-encrypt the
7 streamed content;

8 receiving the encrypted streamed content;

9 simultaneously decrypting and re-encrypting the encrypted content using a
10 combination of the first and the second cipher streams;

11 conveying the re-encrypted content to a sink.

1 13. The medium of Claim 12, wherein the instructions for simultaneously
2 decrypting and re-encrypting the encrypted streamed content comprise instructions
3 which, when executed by the machine, cause the machine to perform further operations

00696864

4 comprising exclusive OR-ing the encrypted streamed content with the cipher stream
5 combination.

1 14. The medium of Claim 12, wherein the cipher stream combination
2 comprises a result of exclusive OR-ing the first and second cipher streams.

1 15. The medium of Claim 12, wherein the first key and the second key have
2 symmetric agreement.

1 16. The medium of Claim 12, further comprising instructions which, when
2 executed by the machine, cause the machine to perform further operations comprising
3 receiving one or more of the first key and the second key over a secure authenticated
4 channel.

1 17. An apparatus comprising:
2 a content interface to receive encrypted streamed content;
3 a computing device to generate a cipher stream based on a first key for
4 encrypted streamed content, to generate a second cipher stream based on a second key to
5 encrypt streamed content and to simultaneously decrypt and re-encrypt the received
6 encrypted streamed content using a combination of the first and the second cipher
7 streams; and
8 a sink interface to convey the re-encrypted content to a sink.

1 18. The apparatus of Claim 17, further comprising a secure authenticated
2 channel interface to receive one of either the first key or the second key.

1 19. The apparatus of Claim 17, wherein the first key and the second key have
2 symmetric agreement and wherein the combination of the first and the second cipher

3 streams is a result of exclusive OR-ing the encrypted content stream with an encryption
4 stream.

1 20. The apparatus of Claim 17, wherein the computing device conveys the
2 second key to the sink to enable the sink to decrypt the re-encrypted content.

1 21. The apparatus of Claim 17, wherein the computing device includes a
2 broadcast entertainment set-top box.

105290" 03E3E260